Chapter 29 - Classified Information Systems

2901 Information Technology Security Requirements

The Department of Commerce requires all operating units to implement and maintain an Information Technology (IT) Security program consistent with the Federal laws and regulations and departmental policies, procedures, and standards. IT Security operations are designed to protect and defend the availability, integrity, and confidentiality of information and information systems. Operating units must establish protection, detection, and reaction capabilities to restore an information system in the event of an intrusion or system failure. Operating units that have a need to process or store classified national security information shall have each IT system certified and accredited prior to processing or storing classified information.

The National Security and Telecommunications Information System Security Instruction No. 1000 (NSTISSI No. 1000) describes the process used to certify and accredit IT systems. The *National Information Assurance Certification and Accreditation Process* (NIACAP) described in this document shall be used as the process for accreditation of classified systems in the Department of Commerce.

2902 Periodic Review of Systems

Systems processing classified national security information shall be reviewed every three years for certification and accreditation or when major changes are made to the system. System owners shall contact the appropriate Designated Approving Authority (see below) to coordinate the review and accreditation process no later than the third anniversary of the original certification (or earlier if necessary) to ensure each system processing classified information is accredited.

2903 Roles and Responsibilities

This paragraph describes the roles and responsibilities of the Department, operating units, program offices, and individuals responsible for safeguarding classified national security information on IT systems processing or storing classified information.

A. Heads of Operating Units. As the system owner, the head of each operating unit is responsible for ensuring that his or her systems are certified and accredited prior to processing or storing classified information. The head of an operating unit shall designate approving authorities and IT Security Officers for his or her organization. The name of the IT Security Officer for each operating unit and/or sub-unit will be submitted in writing through the servicing security officer to the Office of Security. The IT Security Officer shall ensure that system owners properly maintain their respective system's security throughout the system's life cycle.

B. Designated Approving Authority.

1. The head of each operating unit shall appoint one or more Designated Approving Authority (DAA). The DAA has the authority to review and accredit information processing systems in their respective organizations. The DAA will ensure a systems certification team reviews each IT system prior to accreditation. Managers of systems that process classified information shall contact their operating unit's DAA to arrange for system certification and accreditation.

2. The DAA grants formal accreditation to operating systems processing classified national security information. The DAA has the authority to suspend operations, grant interim approval to operate, or approve variances. The approval will be in writing and shall be included in the System Security Plan Certification and Accreditation Package, which is the format used by the Department in place of the Systems Security Authorization Agreement (SSAA) suggested by the National Information Assurance Certification and Accreditation Process (NIACAP).

3. The DAA shall report the findings of security violations and incidents involving classified IT systems to the Director for Security.

C. IT Security Program Manager. The Chief Information Officer is delegated the responsibility to develop Department-wide policies, procedures, and other directives for IT Security, including classified systems. The IT Security Program Manager serves as the principal representative of the Office of the Chief Information Officer to manage and implement the Department's IT Security Program. The IT Security Program Manager provides support to operating units to ensure that IT Security safeguards are planned and implemented throughout the life cycle of the classified IT systems in the Department. The IT Security Program Manager shall perform the following tasks.

1. Provide support to operating units conducting system certification, and support each operating unit's DAA in system accreditation.

2. Review documentation of classified IT systems for completeness and accuracy.

3. Consult with the Office of Security regarding physical and personnel security of classified systems.

4. Ensure that policies and procedures are in place to require security testing and evaluation of classified IT systems in support of the certification process.

5. Establish requirements for the Security Education and Awareness Training program activities pertaining to classified IT systems security.

D. Operating Unit IT Security Officer. The IT Security Officer for each operating unit shall be responsible for assisting the system certification team in collaboration with the Office of Security. The IT Security Officer shall perform the following tasks.

1. Develop and monitor implementation of IT system security policies and procedures for classified systems, including preparation of system security plans and procedures for clearing, purging, declassifying, and releasing system memory, media, and output.

2. Assist in the system's security certification, inspections, tests, and reviews.

3. Ensure that the proper notifications are made and corrective actions are taken when a system incident or vulnerability has been discovered.

4. Investigate security violations and incidents involving classified IT systems and report the findings to the DAA and to the Office of Security.

E. IT System Owner. The IT system owner shall perform the following tasks.

1. Ensure that systems under their responsibility are certified and accredited.

2. Maintain the Systems Security Plan Certification and Accreditation Package (SSPCAP) that includes all system documentation for each classified system.

3. Ensure that all users have the appropriate security clearances and authorization, and that they are

familiar with the system security plan and their security responsibilities prior to receiving access to the information system.

4. Develop an evaluation process to assess changes in a classified IT system and its operating environment and the operational needs that could affect the accreditation.

2904 Additional Requirements

Additional IT Security requirements for classified systems is provided in Chapter 10 of the Information Technology Management Handbook.